



1. Policy for Directed Surveillance and Use of Covert Human Intelligence Sources (CHIS)

Introduction

1. Under Part II of the Regulation of Investigatory Powers Act 2000, authorisation is required before Council Officers can lawfully complete enquiries or investigations that will involve “directed surveillance” or the use of a “covert human intelligence source”.
2. The context of the 2000 Act is the protection of individuals’ fundamental Human Rights now secured by the Human Rights Act 1998. Officers will be aware that in the event of infringement of an individual’s human rights by the Council or its officers, proceedings for compensation are possible under s7 of the 1998 Act: a properly authorised operation will protect the Council from these challenges.
3. When investigating offences, there is a possible danger of Council infringement of the qualified right under Article 8 to respect for private and family life. The intent of the RIPA 2000 is therefore to create a mechanism by which Investigating Authorities can be sure that any directed surveillance or use of covert intelligence sources is lawful and proportionate for the purpose of the 1998 Act.
4. The above aim is achieved by reference to a system of authorisation created by ss27-29 of the RIPA 2000. This policy document seeks to embody the requirements of the 2000 Act in such a way that if authorisations are obtained and used in accordance with the provisions of this document any directed surveillance or use of a CHIS will be lawful. In broad terms the Council’s system for authorisation will require investigating officers to obtain prior written authority for surveillance from a designated RIPA officer within their directorate or unit.

What is Directed Surveillance?

5. “Directed surveillance” will take place in any case where Council Officers observe, listen or record the movements or conversations of individuals as part of a planned investigation in circumstances where the individuals are unaware of the monitoring and the monitoring is likely to result in the Council obtaining information relating to those individuals’ private or family lives.

6. The Officers most likely to be affected by the need for authority for directed surveillance are therefore Housing Benefit Officers investigating suspected benefit fraud. Environmental Health and Planning Enforcement Officers investigating breaches of health regulations and planning control closely related to use of domestic premises may also on occasions be affected by the need to obtain authority under the Act.
7. It should be noted that authority for noise monitoring will not be required in all cases. In particular, where there is no risk of collateral surveillance (see below) and the noise monitoring only produces information relating to db levels or general noise quality there is no requirement for authorisation. More importantly, there will be no requirement for authorisation where the subject is advised of the monitoring. However, authority for noise monitoring in the course of EPA 1990 enquiries will be necessary if the monitoring is covert and is likely to disclose private or family information. It should also be remembered that “private” information is not confined to domestic premises, as the ECHR in Strasbourg has now interpreted the words in a manner that does not exclude business and professional activities.

What is a Covert Human Intelligence Source?

8. As the name suggests, a covert human intelligence source will broadly be a placed informer or a source secretly using a relationship with a third party or a person under investigation for the purpose of obtaining information for use in an investigation.
9. Enquiries involving use of CHIS are not usually undertaken by the Council and are more commonly found in Police enquiries. However Officers should be aware that there may be cases in some licensing enquiries and environmental health enquiries where the Council is in effect making use of a CHIS. For example, the production of log sheets on a covert and long-term basis by third parties in connection with environmental health prosecutions may amount to use of a CHIS.
10. More importantly, personnel investigations of employee misconduct involving covert surveillance and reporting by other Council employees will mean the reporting employees are acting as a CHIS. In such cases the 2000 Act provides that safeguards must be in place relating to use of the information and protecting the welfare of the CHIS.

Collateral Surveillance

11. Investigating officers and authorising RIPA officers need to be particularly mindful of the dangers of collateral surveillance. Collateral surveillance will take place where the Council’s investigations result in the Council obtaining information relating to the private or family lives of individuals other than the surveillance target. In most cases of challenge to directed surveillance the key issue will be chance collateral surveillance causing disproportionate damage to a third party.

12. Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation. An application for an authorisation should include an assessment of the risk of any collateral intrusion. In addition, those carrying out the surveillance should inform the authorising officer if the investigation or surveillance unexpectedly interferes with the privacy of individuals who are not covered by the authorisation.

Intrusive Surveillance

13. If surveillance is planned that involves the presence of a Council Officer or surveillance device on residential premises in circumstances where the owner of the property is the person subject to the investigation and is unaware of the surveillance, the surveillance will be intrusive surveillance for the purposes of the 2000 Act. Intrusive surveillance can only be authorised for the purpose of detecting serious crime and should never be undertaken by the Council.
14. If a Council Officer is contemplating any surveillance that he/she believes may amount to intrusive surveillance, the proposed surveillance must be discussed immediately with either the Monitoring Officer or the Legal Services Manager because this surveillance cannot lawfully be carried out by the Council, with a view to identifying a more suitable method of surveillance.

The Role of RIPA Officers

15. For the purposes of a local authority, directed surveillance and use of a CHIS can only be lawful if authorised by a prescribed officer in writing. In the case of the District Council, officers designated to give authorisations will be known as “RIPA” officers and will have no other subsisting interest in the investigation requiring RIPA authorisation. However if possible, authorisation should be obtained from the RIPA officer within an officer’s own unit or directorate and in all cases the officer considering the request for authorisation should have a day-to-day working knowledge of the issues raised by the proposed directed or CHIS surveillance. In cases where a directorate’s own RIPA officer is non-neutral, authorisation should be obtained direct from the Legal Services Manager or Monitoring Officer.
16. Authority will only be granted if directed surveillance or use of a CHIS is necessary on the following grounds:-
 - (a) For the purpose of preventing or detecting crime and disorder.

Necessity and Proportionality

17. In deciding whether to grant authorisation RIPA officers will first consider whether the directed surveillance or CHIS is necessary or whether alternative non-covert means exist to obtain the evidence. If the evidence can be obtained without directed surveillance or use of a CHIS, authorisation will be refused.

18. The RIPA officer will also consider whether the proposed surveillance and infringement of human rights is proportionate in terms of the object to be achieved by the surveillance. This means that the designated officer will not grant authorisation if he does not consider that the object to be achieved by the surveillance justifies the infringement of the private rights of the individual under investigation.

Officers should consider the following:

- the surveillance should not be excessive in relation to the nature of the operation.
 - whether it is the least invasive method of obtaining information.
 - that collateral intrusion needs to be minimised.
 - that there are regular reviews of the information obtained to check the content.
19. The RIPA officer will also consider the Home Office guidance relating to directed surveillance and the use of CHIS and will seek to limit the risks of collateral surveillance as far as possible. In particular the requirements of s29(5) of the Act and the Source Records Regulations 2000 should be noted. For example, there may be occasions when an officer goes into residential premises with a tape recorder: this would constitute forbidden intrusive surveillance unless the officer has CHIS authorisation and relies on s48(3) which takes the action out of the category of surveillance. The decisions regarding the use of directed surveillance or a CHIS will be recorded on the forms annexed to this policy. The RIPA officer determining the case will then forward a copy of the authorisation to be placed on the central record of authorisations maintained by the Legal Services Manager to the Council.

Reviews, Renewals and Cancellations

20. The role of RIPA officers will not end with a decision on the grant or refusal of authorisation. It is vitally important that any directed surveillance or use of a CHIS is proportionate for the purposes of the investigation only. An authorisation will normally last for a maximum of three months in respect of directed surveillance, and one year in the case of a CHIS. After this time or earlier if a shorter authorisation is considered appropriate by the RIPA officer, the authorisation must either be renewed or cancelled. Authorisation must be cancelled.
21. The request for and outcome of a renewal of authorisation, the formal cancellation of directed surveillance or use of a CHIS will be recorded by means of forms annexed to this policy, forwarded to the Legal Services Manager.
22. When reviewing an authorisation, RIPA officers should consider the issue of timetabling of investigations and endeavour to ensure that directed surveillance does not take place for an excessive time. In many cases review of authorisations will be appropriate within a comparatively short time limit.

23. If at any time before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for a further period of three months. An application for renewal should not be made until shortly before the authorisation period is drawing to an end.
24. The authorising officer who granted or last renewed the authorisation must cancel it if he is satisfied that the directed surveillance no longer meets the criteria upon which it was authorised or is no longer necessary.
25. The final duty of RIPA officers particularly when authorising noise monitoring will be to consider the issue of collateral surveillance with regard to the product of the surveillance. Officers should remember that no offence has been committed under the Environmental Protection until a notice served thereunder has been ignored. For the avoidance of doubt, the best way to address this problem is to hand deliver a notice stating that unless the noise stops, electronic monitoring will be used. This notice makes the operation overt and RIPA irrelevant. If noise monitoring or other directed surveillance has disclosed private information relating to non-target third parties, editing of the product by the authorising officer will usually be appropriate. Once more, it should be noted that “private information” can include that relating to a person’s business and professional activities. However, no information should be edited that could be of use to a defendant in subsequent criminal proceedings and if this requirement raises issues of collateral intrusion the guidance of the Court should be sought at the time of any pleas or directions hearing.

Investigating Officers

26. When completing investigations Officers should at all times be aware of the need to obtain authority for any directed surveillance or use of CHIS. Environmental Health Officers will be required to comply both with the corporate protocol and the unit procedures applying to health authorisations. If the necessary authorisation is not obtained before completing the surveillance, any surveillance will be unlawful raising the possibility of liability on the part of the Council and the Officer responsible for the surveillance.
27. Investigating Officers should also be aware of the broader context of any investigations and enquiries and should ensure at all times that any investigations are authorised within the Council’s general scheme of delegations and are completed with full regard to the civil rights of the individual under investigation, eg. Articles 6 and 8 of the Human Rights Act 1998.

Staff Misconduct

28. Managers should be aware that investigation of staff in respect of employment related misdemeanours as distinct from criminal offences has recently been considered by the Investigatory Powers Tribunal. It has been determined that RIPA Part II does not apply to such cases: however, if it should be considered necessary to place an employee under such surveillance then best practice dictates that the action should be authorised under a quasi-RIPA procedure with the manager in question being under an obligation to justify his/her request.

2. Policy for Accessing Communications Data

Introduction

29. Under Part I of the Regulation of Investigatory Powers Act 2000 the Council can lawfully access “communications data” for certain purposes, including the prevention or detection of crime, by means either of an authorisation issued to a named Council officer or a Notice served on the holder of the data.

Definition of Communications Data

30. For the purposes of the Act “communications data” includes information relating to use of a postal service or telecommunications system but does not include the contents of the communication itself. Home Office guidance indicates communications data comprises three classes of information:-
- (a) “Traffic data”
 - (b) The use made of a communications service by any person, eg. itemised telephone records.
 - (c) Information that is held or obtained by a communications operator or service user, eg. subscriber information.
31. The Home Office defines “traffic data” as information relating to the identity or location of a mobile phone or computer user, or signal routing information.
32. In practical terms the right to communications data will mean that an investigating officer can obtain information about use of post, telephone, email and mobile phone provided a valid authorisation is obtained or Notice served under the Act. Previous use of “communication data” in Council prosecutions is limited to address information arising from postal services. However the new powers under Part I of RIPA will have obvious implications for the detection and investigation of Council Tax and Housing Benefit fraud and could be used to assist in some planning and health enforcement investigations.

Use of Data Acquisition Powers

33. In order to obtain “communications data”, an investigating officer must request authorisation or issue of a Notice from the Legal Services Manager, who is designated as the Council’s authorising officer and single point of contact for the purposes of this part of the Act. The Legal Services Manager will advise regarding the appropriateness of the request and will issue the authorisation or Notice if considered appropriate.
34. If issued an authorisation will provide a legal basis for an investigating officer to collect and retain the communications data for the purpose of the investigation. Authorisation will be appropriate in cases where the postal or telecommunications operator is no longer capable of collecting or retrieving the communications data or if it is believed the investigation will be prejudiced if the operator is asked to collect the data itself.

35. A Notice is served on a postal or telecommunications operator itself in cases where this is the only practicable means of collecting or retrieving the data. In cases where data is obtained by use of a Notice all communications between the service provider and the Council will be channelled through the Legal Services Manager, as single point of contact for the purposes of the Act. A Notice will be in form CD1.
36. There can be no liability on the investigating officer provided an authorisation is obtained or a Notice issued in respect of the communications data required. If communications data is obtained other than through use of the RIPA powers, the investigating officer could be liable to prosecution under the Human Rights Act 1998.
37. In deciding whether to grant an authorisation or issue a Notice it will be necessary for the Legal Services Manager to decide whether use of the Council's powers is necessary and proportionate. By virtue of Section 22(2) of the Act relevant grounds making collection of communications data necessary will include:-
- (i) The interests of public safety.
 - (ii) The protection of public health.
 - (iii) Collection or assessment of any tax, levy or contribution payable to a Government department.
 - (iv) **Preventing or detecting crime.**
 - (v) In an emergency, preventing death or injury or any damage to a person's physical or mental health.
38. The question of proportionality will involve the Legal Services Manager deciding whether any infringement of a human right resulting from use of the powers is justified in view of the objective to be achieved and is not in the circumstances excessive. Use of the powers will most often infringe on an individual's Article 8 right to respect for private life and Protocol 1 Article 1 right to protection of property. Investigating officers should note that due to the importance of human rights' considerations, an authorisation or Notice will not be granted in all cases where it will assist an investigation. Where use of the powers is excessive or disproportionate or if the information could be obtained by another means, the Notice or authorisation would not be granted.

Duration, Renewals and Cancellation

39. Authorisations and Notices will only be valid for one month or such shorter period as is judged proportionate. This period will begin when the authorisation is granted or the Notice is given. An authorisation or Notice may be renewed at any time whilst it is valid by the investigating officer making a renewal application to the Solicitor. More importantly, the investigating officer shall inform the Legal Services Manager once a Notice is no longer necessary or the information is obtained because the Legal Services Manager is then under a duty to cancel the Notice. Home Office guidance also states that Authorisations should be cancelled when they are no longer necessary.

3. Complaints

40. The RIPA 2000 Act establishes an independent Tribunal. The Tribunal has full powers to investigate and decide any case within its jurisdiction. Details of the relevant complaints procedure can be obtained from the following address:

Investigatory Powers Tribunal
PO Box 33220
London SW1H 9ZQ

Tel: 020 7273 4514

RIPA Officers

Strategic Directors
Head of Planning and Building Control
Revenues and Benefits Manager
Legal Services Manager
Environmental Health Managers